CITY OF DURHAM
AUDIT SERVICES DEPARTMENT

Sensitive Information Performance Audit

August 2010

101 City Hall Plaza
Durham, NC 27701
(919) 560-4213

Director of Audit Services
Germaine Brewington, MBA, CPA

Audit Manager
Sonal Patel, CPA, CIA

Senior Auditor
Eric E. Walker, CFE

Auditor
Ora G. Horton, CGAP

DURHAM
1869
CITY OF MEDICINE

CITY OF DURHAM

Memorandum

To: Audit Services Oversight Committee
From: Germaine Brewington, Director of Audit Services
Date: August 16, 2010
RE: Transmittal of Sensitive Information Performance Audit (August 2010)

The Audit Services Department completed the report on the Sensitive Information Performance Audit dated August 2010. The purpose of the audit was to determine if the City is adequately storing and disposing of sensitive information printed on paper documents. In addition, the purpose was to determine if information accessible on City issued Blackberries is secure.

This report presents the observations, results, and recommendations of the Sensitive Information Performance Audit. City management concurs with the recommendations made. Management's response to the recommendations is included with the attached report.

The Audit Services Department appreciates the contribution of time and other resources from the employees of the Human Resources, Housing and Community Development, Finance, Police, Parks and Recreation and General Services Departments in the completion of this audit.

TABLE OF CONTENTS

Sensitive data is privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization/person owning it. In the wrong hands, specific data can provide the necessary information to allow a person to perpetrate identity theft. Laws protect several kinds of information and they require careful handling. Sensitive data includes information such as social security numbers, drivers' license numbers, tax identification numbers, personal health information, financial account numbers, and credit or debit card numbers, in combination with any required security codes, access codes, or passwords that would permit access to an individual's financial account.

City Policy FP 706.03, *"Security of Sensitive and Confidential Information and Breach Response Plan"* addresses managing, maintaining, storing, and disposing of sensitive and confidential information by departments. The purpose of the policy is to respond to the identity theft rules promulgated by the Federal Trade Commission and to attempt to detect, prevent, and mitigate identity theft.

Purpose

The purpose of the audit was twofold:

1) to determine if the City is adequately storing and disposing of sensitive information printed on paper documents; and

2) to determine if information accessible on City issued Blackberries is secure.

We conducted this performance audit in accordance with generally accepted governmental auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

- The City needs to strengthen controls over storing and disposing of sensitive information.
- City staff are adequately securing sensitive information they store, and management provides access to the information on an as needed basis.
- Overall City staff adequately dispose of sensitive information; exceptions were noted in the Police Department.
- City issued Blackberries are not protected to secure access to the contents.

Objectives

The objectives of the audit were to determine if:

- Adequate controls exist over storage and disposition of and access to sensitive information printed on paper documents;
- City staff are adequately storing and disposing of sensitive data and if management is appropriately restricting access to sensitive information contained in paper documents; and
- Proper access controls exist over information contained in City issued Blackberries.

Scope

The scope of the audit included all current practices at the City over storage, disposition of, and access to sensitive information contained in paper documents. The scope also included current practices of access controls over information contained in City issued Blackberries.

Methodology

Audit staff performed the following procedures to verify the objectives of the audit:

- Obtained and reviewed polices/procedures on storing and disposition of sensitive information;
- Surveyed all City departments to determine the nature of sensitive information maintained at each department and the procedures in place to store and dispose of this information. Based on the results of the survey, audit staff selected six departments that maintained the most sensitive information;
- Interviewed employees who either collect, store, have access to, or dispose of sensitive information at six selected City departments;
- Verified if employees are storing sensitive information in a secure environment;
- Verified that access granted to employees is necessary to perform their job;
- Verified if employees are disposing of sensitive information properly by inspecting the contents of the trash collected at the selected departments; and
- Observed employees work areas.

Sensitive information maintained at the six selected departments follows:

Housing and Community Development: Types of sensitive information maintained by the Housing and Community Development Department included: social security numbers, birthdates, tax ID numbers, tax returns, loan status reports, credit reports, credit information, bank account numbers, payroll information, personnel files, income statements, and bank statements.

Finance: The Finance Department collected various types of sensitive information, which included but was not limited to: social security numbers, credit card numbers, bank and credit union account numbers, employee payroll data, bank routing numbers, tax ID numbers, and employment information.

General Services: Sensitive information collected by the General Services staff included: social security numbers, birthdates, employee numbers, and drivers' license numbers.

Human Resources: The Human Resources Department collected many types of sensitive information including but not limited to: social security numbers, credit card numbers, bank and credit union account numbers, health insurance plan identification numbers, drivers' license numbers, birthdates, and other similar information associated with a job applicant or employee.

Parks and Recreation: Sensitive information maintained within the Parks & Recreation Department included: social security numbers, birthdates, credit card numbers, medical information, background checks, W2's, W4's and employee personnel information.

Police: Sensitive information maintained at the Police Department included: social security numbers, birthdates, addresses, credit card numbers, disciplinary information, bank account information, medical information, polygraph exams, drivers' histories, background investigations, psychological results, training files, narratives from crime scenes, and other documents covered by the Personnel Privacy Act.

The results of the audit are:

The City needs to strengthen controls over storing and disposing of sensitive information.

Policy FP 706.03 *"Security of Sensitive and Confidential Information and Breach Response Plan"* provides guidance on how departments should maintain store, and dispose of sensitive information. In addition, it also places the responsibility on department directors for determining employees that should access and handle sensitive and confidential information.

According to Policy FP 706.03, each department will develop and maintain a standard procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. In five of the six departments tested, written standard procedures to provide staff with specific guidance on the protection of sensitive and confidential information did not exist.

The Department of Housing and Community Development maintains an offsite storage facility. Access to the storage facility is limited to the Fiscal Program Accountant and the Budget and Management Analyst. Procedures to ensure periodic inspection of the offsite facility and to ensure documents are intact did not exist. Housing and Community Development staff indicated that efforts have recently been implemented to correct this. Departments that utilize offsite storage facilities should also address controls to protect sensitive information at the offsite location in its written standards - specifically, periodically inventorying and ensuring all stored items are present.

City staff are adequately securing sensitive information they store and management provides access to the information on an as needed basis.

Departments store paper documents that contain sensitive information either in central filing storage areas within the office or employees maintain sensitive information in secure file cabinets in their respective offices. Some departments utilize an offsite storage facility to house information that requires long-term retention. The six selected departments adequately secure sensitive information. Employees at the selected departments maintain sensitive information with care and store it securely. Employees lock file cabinets and do not leave sensitive information on their desks. Employees lock office doors when they step away from their desks during the course of the day. In addition, personnel are given access to sensitive data when it is required to carry out one's job responsibilities.

Overall City staff adequately dispose of sensitive information; exceptions were noted in the Police Department.

Five of the six selected departments take reasonable measures when destroying sensitive data that will prohibit the information from being read or reconstructed. The identified individuals who had possession/access to sensitive paper documents shredded the documents with sensitive data. Employees of the six selected departments had access to shredders. On two separate occasions, audit staff examined trash collected by the General Services custodial staff to determine if sensitive information was being disposed of in the trash rather than being shredded. The examination revealed a few documents containing sensitive information such as date of birth, name and drivers' license information in the trash of the Police Department. In addition, during the same period, janitorial staff found documents containing social security numbers in the recycling bin of the Police Department. The documents were returned to Police Department personnel for proper disposition. Disposing of sensitive information in recycling bins is not an appropriate practice.

City issued Blackberries are not protected to secure access to the contents.

Technology Solutions staff examined Blackberries issued to fifty-one (51) City employees to determine if the password protection function was on. Of the fifty-one (51) Blackberries issued, only fourteen (14) employees had password protection enabled.

Recommendation 1

As required by Policy FP 706.03, all City departments should:

- Develop and maintain a standard operating procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. The procedures should also address controls to ensure inventory is monitored at offsite storage facilities; and
- Inform its employees of Policy FP 706.03.

Recommendation 2

The Housing and Community Development Department should periodically inventory the information stored in the offsite storage facility. In addition, the Department staff should periodically visit the offsite storage facility to ensure records are not compromised.

Recommendation 3

The Police Department should ensure that staff are properly following the guidance as required by Policy FP 706.03 regarding the disposition of sensitive and confidential information.

Recommendation 4

The Technology Solutions Department should ensure that all City issued Blackberries are protected against unauthorized access to sensitive information utilizing passwords or some other effective means.

Memorandum

DURHAM
CITY OF DURHAM
1869
CITY OF MEDICINE

To: Thomas J. Bonfield, City Manager

From: Wanda S. Page, Deputy City Manager

Date: September 2, 2010

Subject: **Management's Response to the Sensitive Information Audit (August, 2010)**

The following is management's response to the recommendations contained in the Sensitive Information Audit dated August 2010.

Recommendation #1: (All City Departments)
As required by Policy FP 706.03, all City departments should:

- Develop and maintain a standard operating procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. The procedures should also address controls to ensure inventory is monitored at offsite storage facilities; and
- Inform its employees of Policy FP 706.03.

Management's Response:

We concur.

City Policy, FP 706.03 - *Security of Sensitive and Confidential Information and Breach Response Plan,* effective August 1, 2009 requires each department to maintain a standard procedure to provide staff with specific guidance on the protection of sensitive and confidential information that is specific to that department. In order to ensure that Department's have developed, implemented, and documented their procedures, the City Manager's Office will obtain and inspect for sufficiency the written procedures of each Department that maintains sensitive and confidential information by December 31, 2010.

FP 706.03 was implemented in August 2009, distributed to all departments and posted to the City's intranet in the "policies" section to provide direction to departments and employees. Departments will be sent a reminder to review and implement all policy requirements and progress will be monitored.

Recommendation #2: (Housing and Community Development)
The Housing and Community Development Department should periodically inventory the information stored in the offsite storage facility. In addition, the Department staff should periodically visit the offsite storage facility to ensure records are not compromised.

Management's Response:

We concur.

The Department of Community Development has implemented a procedure responsive to this recommendation.

Off-Site Storage Inspection Procedures- Internal Control Policy DCD 101.00
The Department of Community Development (DCD) will use the following procedures to inspect the off-site storage facility to ensure that records are managed, secured and stored in accordance with City Policy FP 706.03.

The DCD's inactive records are maintained according to the City's Record Retention Policy and other legal or regulatory requirements. Inactive records stored at the off-site storage facility are secured in a climate-controlled storage unit and access is limited to DCD's Fiscal Program Accountant and the Business Services Manager.

The DCD Fiscal Management Division will be responsible for:

a. Transferring records to and from the off-site storage facility.
b. Maintaining an inventory of records stored at the off-site storage facility.
c. Conducting a monthly visit to the off-site storage facility to ensure that stored documents have not been compromised and the unit is secure.
d. Conducting an annual file review to identify records that have reached their legal or regulatory retention period and prepare them for destruction. A list of the discarded records will be noted and maintained in the DCD records retention file and also posted on the DCD K-Drive (k:\Record Retention). The DCD Compliance and Monitoring Officer will maintain these records.

Recommendation #3: (Police Department)
The Police Department should ensure that staff are properly following the guidance as required by Policy FP 706.03 regarding the disposition of sensitive and confidential information.

Management's Response:

We concur.

All Police Department employees will be required to read City Policy FP 706.03, the Department's new General Order related to the Security of Sensitive and Confidential Information, their respective SOPs related to the subject and sign the City's Sensitive Information User Agreement which will be maintained in their employee file. The target date for having this completed is October 30, 2010.

Recommendation #4: (Technology Solutions)
The Technology Solutions Department should ensure that all City issued Blackberries are protected against unauthorized access to sensitive information utilizing passwords or some other effective means.

Management's Response:

We concur.

The Technology Solutions Department will work to reduce the risk that City issued Blackberries will provide access to sensitive information by updating employee use policies, implementing passwords or utilizing other effective means to obtain this outcome. Solutions will be finalized by December 31, 2010.

CC: Germaine Brewington, Director of Internal Audit
Kerry Goode, Director of Technology Services
Jose L. Lopez, Sr., Chief of Police
Diana Monaco, RPA, CM, Assistant Director Department of Community Development